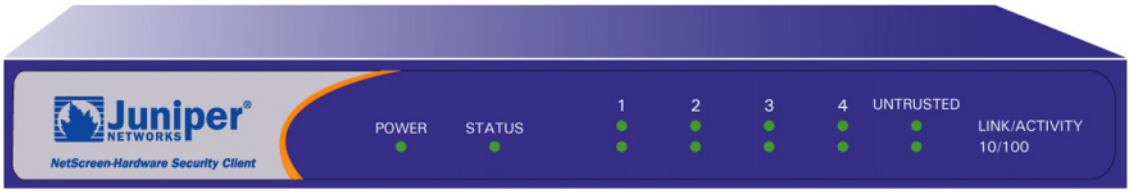
NETSCREEN-HARDWARE SECURITY CLIENT

User's Guide

Version 5.0 P/N 093-1308-000 Rev B



Copyright Notice

Copyright © 2004 Juniper Networks, Inc. All rights reserved.

Juniper Networks, the Juniper Networks logo, NetScreen, NetScreen Technologies, GigaScreen, and the NetScreen logo are registered trademarks of Juniper Networks, Inc. NetScreen-5GT, NetScreen-5XP, NetScreen-5XT, NetScreen-25, NetScreen-50, NetScreen-100, NetScreen-204, NetScreen-208, NetScreen-500, NetScreen-5200, NetScreen-5400, NetScreen-Global PRO, NetScreen-Global PRO Express, NetScreen-Remote Security Client, NetScreen-Remote VPN Client, NetScreen-IDP 10, NetScreen-IDP 100, NetScreen-IDP 500, GigaScreen ASIC, GigaScreen-II ASIC, and NetScreen ScreenOS are trademarks of Juniper Networks, Inc. All other trademarks and registered trademarks are the property of their respective companies.

Information in this document is subject to change without notice.

No part of this document may be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose, without receiving written permission from:

Juniper Networks, Inc.

ATTN: General Counsel

1194 N. Mathilda Ave.Sunnyvale, CA 95014

FCC Statement

The following information is for FCC compliance of Class A devices: This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. The equipment generates, uses, and can radiate radio-frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference, in which case users will be required to correct the interference at their own expense.

The following information is for FCC compliance of Class B devices: The equipment described in this manual generates and may radiate radio-frequency energy. If it is not installed in accordance with NetScreen's installation instructions, it may cause interference with radio and television reception. This equipment has been tested and found to comply with the limits for a Class B digital device in accordance with the specifications in part 15 of the FCC rules. These specifications are designed to provide reasonable protection against such interference in a residential installation. However, there is no guarantee that interference will not occur in a particular installation.

If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Consult the dealer or an experienced radio/TV technician for help.
- Connect the equipment to an outlet on a circuit different from that to which the receiver is connected.

Caution: Changes or modifications to this product could void the user's warranty and authority to operate this device.

Disclaimer

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR NETSCREEN REPRESENTATIVE FOR A COPY.

Contents

Preface v

Organization v

CLI Conventions v

Juniper Networks NetScreen Publications vi

Chapter 1 Connecting the Device 1

Connecting to the Network 1

Connecting the Power 1

Chapter 2 Configuring the Device 3

About Default Settings 4

Accessing the Device 6

Configuring the Device 7

Verifying External Connectivity 11

Restoring Default Settings 11

Chapter 3 Managing the Device 13

Centralized Management 13

Local Management 13

AntiVirus Scanning 14

Chapter 4 Hardware Descriptions 15

Port and Power Connectors 15

Status LEDs 15

Appendix A Specifications A-1

Preface

The Juniper Networks NetScreen-Hardware Security Client provides IPSec VPN and firewall services for a broadband telecommuter, a branch office, or a retail outlet. The NetScreen-Hardware Security Client uses the same firewall, VPN, and traffic management technology as NetScreen's high-end central site products.

ORGANIZATION

This guide has four chapters and one appendix:

- Chapter 1, "Connecting the Device" describes how to connect the NetScreen-Hardware Security Client to the network and a power source.
- Chapter 2, "Configuring the Device" describes how to access and configure the NetScreen-Hardware Security Client.
- Chapter 3, "Managing the Device" describes the management options for the NetScreen-Hardware Security Client, including how to enable AntiVirus Scanning.
- Chapter 4, "Hardware Descriptions" describes the NetScreen-Hardware Security Client chassis.
- Appendix A, "Specifications", provides general system specifications for the NetScreen-Hardware Security Client.

CLI CONVENTIONS

The following conventions are used when presenting the syntax of a command line interface (CLI) command:

- Anything inside square brackets [ ] is optional.
- Anything inside braces { } is required.
- If there is more than one choice, each choice is separated by a pipe (|). For example,

  ```
  set interface { ethernet1 | ethernet2 | ethernet3 }
  manage
  ```

  means "set the management options for the ethernet1, ethernet2, or ethernet3 interface".
- Variables appear in *italic*. For example:

  set admin user *name1* **password** *xyz*

When a CLI command appears within the context of a sentence, it is in **bold** (except for variables, which are always in *italic*). For example: “Use the **get system** command to display the serial number of a NetScreen device.”

*Note: When typing a keyword, you only have to type enough letters to identify the word uniquely. For example, typing **set adm u joe j12fmt54** is enough to enter the command **set admin user joe j12fmt54**. Although you can use this shortcut when entering commands, all the commands documented here are presented in their entirety.*

JUNIPER NETWORKS NETSCREEN PUBLICATIONS

To obtain technical documentation for any Juniper Networks NetScreen product, visit www.netscreen.com/resources/manuals/.

To obtain the latest software version, visit: www.netscreen.com/services/download_soft. Select a category of software product from the dropdown list, then follow the displayed instructions. (You must be a registered user to download Juniper Networks Netscreen software.)

If you find any errors or omissions in the following content, please contact us at the e-mail address below:

techpubs@netscreen.com

1

Connecting the Device

This chapter describes how to connect the Juniper Networks NetScreen-Hardware Security Client to the network and a power source.

Note: For safety warnings and instructions, refer to the NetScreen Safety Guide. *The instructions in the Safety Guide warn you about situations that could cause bodily injury. Before working on any equipment, be aware of the hazards involved with electrical circuitry and be familiar with standard practices for preventing accidents.*

Connecting to the Network

To enable the NetScreen-Hardware Security Client to provide firewall and general security for your network, you must connect the Untrusted port to the Internet and the Trusted ports to your internal network.

Connecting the Untrusted Port

The Untrusted port handles traffic between the device and the Internet or other outside computers. The NetScreen-Hardware Security Client contains one Untrusted port that you can use to connect to an external router, DSL modem, or cable modem. To connect the device to the Internet, use the provided Ethernet cable between the Untrusted port on the device and an external router or modem.

Connecting the Trusted Ports

A Trusted port handles traffic between the device and your internal workstations. The NetScreen-Hardware Security Client contains four Trusted ports that you can use to connect LANs or workstations:

- To connect the device to a LAN via an internal switch or hub, use an Ethernet cable between a Trusted port and a port on the switch or hub.
- To connect the device directly to a workstation, use an Ethernet cable between a Trusted port and the workstation Ethernet port.

Connecting the Power

To connect a power source to the NetScreen-Hardware Security Client device:

1. Plug the DC connector end of the power cable into the DC power receptacle on the back of the device.
2. Plug the AC adapter end of the power cable into an AC power source.

Warning: *Juniper Networks recommends using a surge protector for the power connection.*

2 Configuring the Device

This chapter describes how to access and configure a Juniper Networks NetScreen-Hardware Security Client.

Before you configure the device, ensure that you have connected it to your network and to a power source as detailed in "Connecting the Device" on page 1.

After completing the device configuration, your network users can access the Internet through the Juniper Network device while resources in your network are protected from outside computers. The Juniper Networks device includes a default policy that permits your network workstations to use any service to access outside computers and denies outside computers access to your network workstations.

To configure additional policies that direct the Juniper Networks device to permit outside computers to start specific kinds of sessions with your computers, you must use NetScreen-Security Manager 2004 or ScreenOS CLI commands:

- For details on firewall policies in NetScreen-Security Manager, see the "Configuring Firewall Policies" chapter in the *Juniper Networks NetScreen-Security Manager 2004 Administrator's Guide*.
- For details on VPN policies in NetScreen-Security Manager, see the "Configuring VPN Policies" chapter in the *Juniper Networks NetScreen-Security Manager 2004 Administrator's Guide*.
- For details on creating or modifying policies with ScreenOS CLI commands, see the *NetScreen Concepts & Examples ScreenOS Reference Guide*.

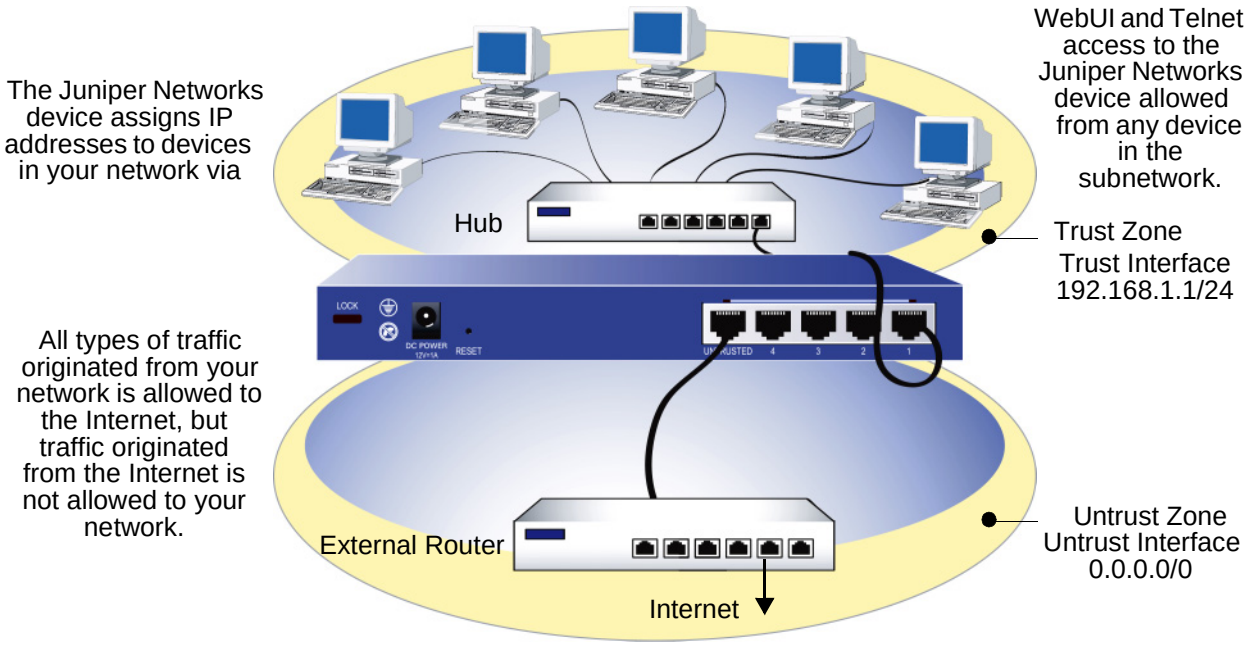
Note: *You cannot create firewall policies or VPNs using the NetScreen-Hardware Security Client WebUI.*

After you configure the device, you should verify that the device is working correctly (for details, see "Verifying External Connectivity" on page 11).

If you experience problems completing a configuration, you can restore the device to its default settings (for details, see "Restoring Default Settings" on page 11).

About Default Settings

The NetScreen-Hardware Security Client includes pre-defined, default settings:


The Juniper Networks device assigns IP addresses to devices in your network via
WebUI and Telnet access to the Juniper Networks device allowed from any device in the subnetwork.
Hub
Trust Zone
Trust Interface
192.168.1.1/24
All types of traffic originated from your network is allowed to the Internet, but traffic originated from the Internet is not allowed to your network.
External Router
Untrust Zone
Untrust Interface
0.0.0.0/0
Internet

Typically, you need to change only a few default settings to make your device operational on your network. Some settings are *required*, meaning you must change the default values to values that are relevant for your network before the device is operational. Other settings are *optional*, meaning you can use the pre-defined default values.

This guide does not describe optional settings; for details on configuring an optional setting, see the appropriate sections in the *NetScreen Concepts & Examples ScreenOS Reference Guide*.

The following sections detail the information you will need to configure the device.

Untrust Interface Address (Required)

The Untrust interface is bound to the Untrust zone and is configured with the IP address 0.0.0.0/0. You must configure an IP address for the Untrust interface to enable the Juniper Networks device (and the workstations on your network) to connect to the Internet. This IP address represents your network to the outside world and is obtained from your Internet Service Provider (ISP) in one of the following ways:

- You receive a specific, fixed IP address and netmask for your network from your Internet Service Provider (ISP).
- Your network receives an IP address from a server via Dynamic Host Configuration Protocol (DHCP).
- Your network receives an IP address from a server via Point-to-Point Protocol over Ethernet (PPPoE).

Admin Name & Password (Required)

Any user in the subnetwork who knows the device admin name and password can access and configure the Juniper Networks device. Because all Juniper Networks FW/VPN devices use the same default admin name and password (netscreen, netscreen), Juniper Networks highly recommends that you change your login and password to the Juniper Networks device.

Port Mode (Optional)

The *port mode* is the binding of physical ports, logical interfaces, and zones. The default port mode, Trust-Untrust, binds the Trust interface to the Trust zone and the Untrust interface to the Untrust zone. Changing the port mode changes these bindings.

This guide details how to configure your device in the Trust-Untrust port mode only. For details on port modes and how to change them, see the "Zones" chapter in Volume 2 of the *NetScreen Concepts & Examples ScreenOS Reference Guide*.

Warning: *Because changing the port mode removes any existing configurations on the Juniper Networks device, you should change the port mode before configuring the device.*

Management (Optional)

You can configure the following management settings:

- Specify the connection protocol (Telnet, SSH) that a host can use to communicate with the device.
- Specify the communication parameters that enable the device to connect to NetScreen-Security Manager 2004 for management.

For details, see the "Administration" chapter in Volume 3 of the *NetScreen Concepts & Examples ScreenOS Reference Guide.*

Operational Mode (Optional)

The *operational mode* defines how your device operates with its connected networks. By default, the NetScreen-Hardware Security Client operates in Route mode with Network Address Translation (NAT) enabled on the Trust interface. In this operational mode, when workstations in the Trust zone send traffic to the Internet, the device replaces the original source IP addresses with the IP address of the Untrust interface. Because the device assigns private IP addresses to your network workstations, these addresses are never seen by computers outside your network.

For details on configuring the device for Route mode without NAT enabled, see the "Interface Modes" chapter in Volume 2 of the *NetScreen Concepts & Examples ScreenOS Reference Guide*

Note: *The NetScreen-Hardware Security Client does not support Transparent mode.*

Trust Interface Address (Optional)

The Trust interface is bound to the Trust zone and is configured with the subnetwork address 192.168.1.1/24. All workstations that you connect to the Trust interface must be in the same subnetwork and have IP addresses in that subnetwork. The NetScreen-Hardware Security Client can also use DHCP to automatically assign IP addresses for the 192.168.1.1/24 subnetwork to your network workstations.

You might need to change the IP address and netmask of the Trust interface to match the IP addresses that already exist on your network. If you do change the Trust IP, you must also change the range of addresses that the DHCP server assigns to your network workstations, or disable the DHCP server on the Trust interface.

For details on assigning a different IP address and netmask to the Trust interface, see the "Interfaces" chapter in Volume 2 of the *NetScreen Concepts & Examples ScreenOS Reference Guide*.

For details on changing the DHCP settings for the Juniper Networks device, see the "System Parameters" chapter in Volume 2 of the *Juniper Networks NetScreen Concepts & Examples ScreenOS Reference Guide*.

ACCESSING THE DEVICE

Before you attempt to access the device, ensure that you have connected it to your network and to a power source. You can access the NetScreen-Hardware Security Client using one of the following methods:

- **Rapid Deployment**, a method for configuring a Juniper Networks device for management by NetScreen-Security Manager 2004, an integrated management system for all Juniper Networks FW/VPN devices. In the Rapid Deployment process, the NetScreen-Security Manager administrator generates a small configuration file (called a configlet) in the management system, then sends the configlet to the on-site administrator, who uses the configlet to automatically configure the device. For details and step-by-step instructions on using Rapid Deployment to configure your device, see the *Getting Started Guide* for the NetScreen-Hardware Security Client.
- **WebUI**, a graphical user interface that enables you to access the device through a Web browser. To use the WebUI, you must be on the same subnetwork as the device.
- **Telnet**, a command line application that enables you to access the device through an IP network. To access and configure the device, you use ScreenOS Command Line Interface (CLI) commands in a Telnet session from your workstation. You can also access remote Juniper Networks devices using Secure Shell (SSH) applications. For details on using SSH, see the Administration volume of the *NetScreen Concepts & Examples ScreenOS Reference Guide*.

Note: *The NetScreen-Hardware Security Client does not have a console port.*

CONFIGURING THE DEVICE

You can configure the required device settings using Rapid Deployment, the WebUI or CLI commands via a Telnet connection. For a required setting, you must change the default value to a value that is relevant for your network before the device is operational.

> ***Note:*** *This guide does not describe optional settings; for details on configuring an optional setting, see the appropriate sections in the* Juniper Networks NetScreen Concepts & Examples ScreenOS Reference Guide.

The instructions below detail how to configure your device using the WebUI or CLI command via Telnet. For instruction on using Rapid Deployment to configure the device, see the *Getting Started Guide* for the NetScreen-Hardware Security Client.

If you experience problems completing a configuration, you can restore the device to its default settings (see "Restoring Default Settings" on page 11). To troubleshoot basic device problems, see the *NetScreen-Hardware Security Client Administrator's Guide*.

Using the WebUI

You can configure the device using the WebUI Initial Configuration Wizard. To use the WebUI, you must be on the same subnetwork as the Juniper Networks device.

Accessing the Device

To access the NetScreen-Hardware Security Client device using the WebUI:

1. Connect a workstation (or your LAN hub) to the Trusted ports, as described in "Connecting to the Network" on page 1.
2. Configure the workstation to be on the same subnet as the device using one of the following methods:
   - *Using DHCP*. Configure your workstation to automatically receive an IP address from the Juniper Networks device using DHCP (ensure that your internal network does not already use a DHCP server).
   - *Using a Static IP address*. Configure your workstation to use a static IP address that is on the 192.168.1.0 network.

   For help, see your PC operating system documentation.
3. If necessary, restart your workstation. Some operating systems must be restarted before new settings can take effect.
4. Launch a Web browser, type the IP address for the Trust interface in the URL field, and then press **Enter**. After a few moments, the Initial Configuration Wizard appears.

   Example: If the IP address of the Trust interface on the Juniper Networks device is 192.168.1.1/24, type the following: **192.168.1.1**

Using the Wizard

To configure the device using the WebUI, follow the instructions in the Initial Configuration Wizard. This wizard appears when you access the WebUI for the first time, and helps you configure the default settings on the device:

1. Select **No, use the Initial Configuration Wizard instead**, and then click **Next** to continue.

   If you have received a configlet from your NetScreen-Security Manager administrator to help you configure the device, do not continue to use the instructions below. Please see the *Getting Started Guide* for the NetScreen-Hardware Security Client for details on using a configlet for Rapid Deployment.

   If you want to skip the Wizard and go directly to the WebUI to configure the device, then select **No, skip the Wizard and go straight to WebUI management session**.

2. Select **No Plain Configuration File**, and then click **Next** to continue. The Initial Configuration Welcome screen appears. click **Next** to continue.
3. Check the **Enable NAT** check box if you want the device to be in Route mode with NAT enabled. Click **Next** to continue.
4. Type the device admin name and password. Click **Next** to continue.
5. Type the information that describes how your device connects to the Internet:
   - If your device uses DHCP to obtain an IP address for the Untrust zone interface, select **Dynamic IP via DHCP**.
   - If your device uses a PPPoE connection to obtain an IP address for the Untrust zone Interface, select **Dynamic IP via PPPoE**. Selecting this option enables your Juniper Networks device to act as a PPPoE client that can receive an IP address for the Untrust zone interface from an ISP. Type the username and password for your PPPoE account.
   - If your device uses a static IP address for the Untrust zone interface, select **Static IP**. Selecting this option enables your Juniper Networks device to use a unique and fixed IP address for the Untrust zone interface. Type the IP address, Netmask, and Gateway for the device.

     The IP address is the IP address of the interface that is connected to the external router, cable modem, or DSL modem. The gateway address is the IP address of the router port connected to the Juniper Networks device.

   Click **Next** to continue.
6. Configure the IP address of the Trust zone interface:
   - To use the existing IP address, simply click **Next**.
   - To change the existing IP address, type the new IP address and netmask, then click **Next**.

If you change the IP address and netmask of the Trust zone interface, your PC and the Trust interface of the Juniper Networks device may then be on different subnetworks. To continue managing the Juniper Networks device through the WebUI, ensure that both your PC and the Juniper Networks device are in the same IP network and use the same netmask.

7. Configure DHCP for the Trust zone interface:
   - **Yes**, If using NAT mode, enable DHCP to automatically assign IP addresses to workstations in the Trust zone.
   - **No**, If using Route mode, disable DHCP.

   Click **Next** to continue.

8. Configure the management system for the device:
   - Select **Yes** to configure the device to connect to NetScreen-Security Manager. Click **Next** to continue and go to step 9.
   - Select **No** to configure the connection protocols for the device, but not connect to NetScreen-Security Manager. Click **Next** to continue and goto step 10.

9. Type the communication parameters that enable the device to connect to NetScreen-Security Manager:
   - **Security Manager Address**. Type the IP address of the Security Manager device-server (provided by the Security Manager administrator).
   - **Device ID**. Type the device ID of the device (provided by the Security Manager administrator).
   - **One Time Password**. Type a one time password. When the device connects to Security Manager, the one time password authenticates the initial connection.
   - **Port Number**. Type the port number on the Security Manager device-server (provided by the Security Manager administrator).
   - **Admin Name**. Type the name of the device admin.
   - **Admin Password**. Type the password of the device admin.

   Click **Next** to display the configuration summary and goto step 11.

10. Configure the connection protocols for the device untrusted port. You can enable one or both protocols.
    - **SSH**. To access and manage the device remotely using SSH, you must enable SSH on the device untrusted port.
    - **Telnet**. To access and manage the device remotely using Telnet, you must enable Telnet on the device untrusted port.

    Click **Next** to display the configuration summary.

11. Review the configuration information:
    - Click **Previous** to re-type configuration information.
    - Click **Next** to type the configuration.

After you have configured the device, a confirmation screen appears.

- To verify that the device has connectivity to the Internet, see "Verifying External Connectivity" on page 11.
- To use the WebUI to view or change the device configuration, open a Web browser and type the IP address for the Trust interface in the URL field. At the login prompt, type the device admin name and password and click **Enter** to display the WebUI.
- To restore the default device settings on the device, see "Restoring Default Settings" on page 11.

Using Telnet

You can access and configure the device using ScreenOS CLI commands. Follow the instructions in the sections below to change the required settings for the device.

Accessing the Device

To access the device:

1. Connect your workstation (or your LAN hub) to the Trusted ports, as described in "Connecting to the Network" on page 1.
2. Start a Telnet client application to the IP address for the Trust interface. For example, if the IP address of the Trust interface on the Juniper Networks device is 192.168.1.1/24, type the following: **192.168.1.1**
3. Type **netscreen** in both the **admin name** and **password** prompts. (Use lowercase letters only. The admin name and password fields are both case sensitive.)

Configuring the Untrust Interface

Your network uses the Untrust interface on the Juniper Networks device to connect to the Internet. If you are setting up your Internet connection for the first time, contact your ISP for information on your network IP address assignment.

In a Telnet session:

- If your ISP gave you a specific, fixed IP address and netmask for your network, configure the IP address and netmask for the network and the IP address of the router port connected to the Juniper Networks device by typing the following CLI commands:

```
set interface untrust ip ip_addr/mask
set interface untrust gateway ip_addr
save
```

- If your network receives an IP address from a server via DHCP, enable the DHCP client by typing the following CLI commands:

```
set interface untrust dhcp client enable
save
```

- If your network receives an IP address from a server via PPPoE, configure the user name and password assigned by your ISP by typing the following CLI commands:

```
set pppoe interface untrust
set pppoe username name_str password pswd_str
save
```

Configuring Admin Name & Password

Because all Juniper Networks NetScreen products use the same default admin name and password (**netscreen**), you should change the default admin name and password immediately.

In a Telnet session, type the following CLI commands:

```
set admin name name_str
set admin password pswd_str
save
```

For information on creating different levels of administrators, see the "Administration" chapter in Volume 3 of the *NetScreen Concepts & Examples ScreenOS Reference Guide*.

VERIFYING EXTERNAL CONNECTIVITY

After you have configured the device, you should verify that workstations in your network can access resources on the Internet. To verify, start a Web browser from any workstation in the network and type the following URL: www.juniper.net.

To troubleshoot basic device problems, see the *NetScreen-Hardware Security Client Administrator's Guide*.

RESTORING DEFAULT SETTINGS

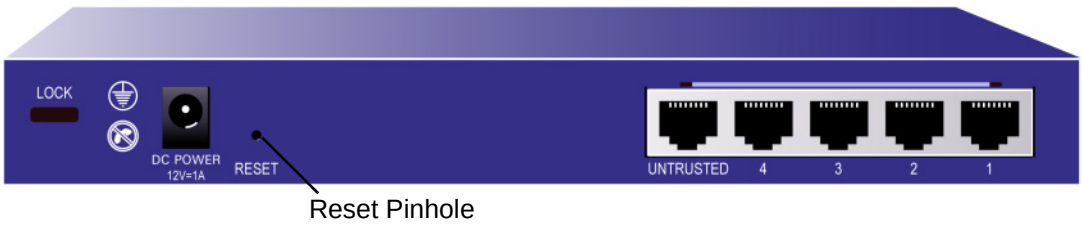
You can restore the factory default configuration of the device. Although resetting the device destroys all existing configuration, it safely restores access to the device. You might need to restore defaults:

- If you experience problems during device configuration
- If you lose the admin password
- If you want to configure a device using Rapid Deployment. For details, see the *Getting Started Guide* for the NetScreen-Hardware Security Client.

Warning: *Resetting the device deletes all existing configuration settings and renders existing firewall and VPN service inoperative.*

To restore the device to its default settings:

1. Locate the reset pinhole on the back panel. Using a thin, firm wire (such as a paper clip), push the pinhole until the Status LED turns from blinking green to orange, and then back to blinking green. Release the pinhole.



2. Wait for four seconds.
3. Push the reset pinhole again. When the Status LED turns to red, and then to green, release the pinhole.
4. The device resets to its original factory settings and restarts. After the device starts up (should take about 30 seconds), ensure that the Power LED and Status LED both blink green.

If you do not follow the complete sequence, the reset process cancels without changing the configuration, and the Status LED blinks green. If the device did not reset, an SNMP alert is sent to confirm the failure.

3 Managing the Device

This chapter describes the management options for your Juniper Networks NetScreen-Hardware Security Client and details the antivirus scanning feature.

After you have connected the device to your network and configured it, you can begin using centralized or local management to control device functionality.

CENTRALIZED MANAGEMENT

Your NetScreen-Hardware Security Client is designed to be managed using Netscreen- Security Manager 2004, an integrated management system for all NetScreen FW/VPN devices. For details on using NetScreen-Security Manager to manage your NetScreen FW/VPN devices, see the *NetScreen-Security Manager 2004 Administrator's Guide*.

LOCAL MANAGEMENT

You can use the WebUI or ScreenOS CLI commands (using Telnet or SSH) to manage the NetScreen-Hardware Security Client.

WebUI

The WebUI is a graphical user interface that enables you to manage the device using a Web browser. To use the WebUI, you must be on the same subnetwork as the device.

You can use the WebUI to manage specific device functionality:

- Configure basic device settings
- View the device configuration
- Monitor system, firewall, and VPN status
- Monitor system, firewall, and VPN events
- Configure the device for management by NetScreen-Security Manager 2004

To manage additional device functionality, you must use NetScreen-Security Manager or ScreenOS CLI commands.

CLI

ScreenOS Command Line Interface (CLI) commands enable you to manage the device in a Telnet or Secure Shell (SSH) session.

You can use CLI commands to manage all device functionality. For details on ScreenOS CLI commands, see the *NetScreen CLI Reference Guide*.

ANTIVIRUS SCANNING

Your device includes internal antivirus scanning to detect viruses in specific application-layer transactions. When antivirus scanning is enabled, the device uses an internal antivirus scan engine developed by TrendMicro to examine SMTP, HTTP (webmail only) or POP3 traffic for known virus patterns.

By default, the device automatically passes all permitted SMTP, HTTP, and POP3 traffic to the internal antivirus scan engine. After verifying that it has received the entire content of the packet, the internal antivirus scan engine examines the data for viruses:

- If a virus is detected, the device drops the content and sends a message to the client indicating that the content was infected.
- If no virus is detected, the device forwards the content to its intended destination.

The antivirus scan engine can examine up to 16MB of concurrent messages. If the total size of messages received concurrently exceeds this amount, the scan engine bypasses the content (does not scan it). For example, the internal antivirus scan engine can receive and examine four-4MB messages concurrently. If the internal antivirus scan engine receives 17-1MB messages concurrently, it would drop or pass the traffic depending on content. For HTTP traffic scanning, the device can redirect Web server responses to the internal antivirus scan engine before forwarding the traffic to the client.

For details on the antivirus scan engine, see the AntiVirus Scanning section in Volume 4 (Attack Detection and Defense Mechanisms) of the *NetScreen Concepts & Examples ScreenOS Reference Guide*.

4

Hardware Descriptions

This chapter details the Juniper Networks NetScreen-Hardware Security Client chassis.

Port and Power Connectors

The rear panel of the NetScreen-Hardware Security Client contains port and power connectors.

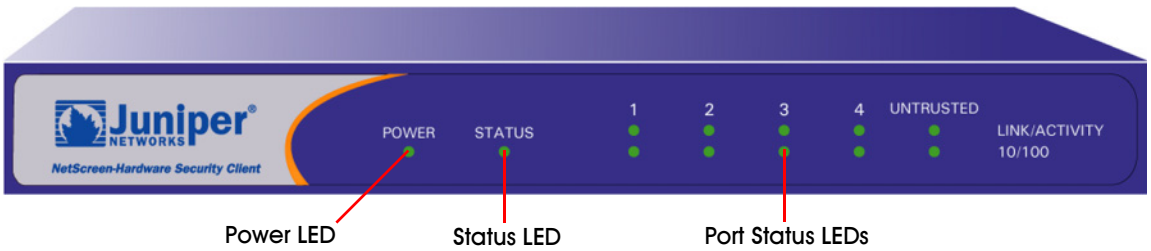
- Use the DC power receptacle to connect the device to a power source
- Use the Reset pinhole to reset the device and restore its factory default settings.

The NetScreen-Hardware Security Client includes the following ports:

Port	Description	Connector	Speed/Protocol
Untrusted	Enables an Internet connection through an external router, DSL modem, or cable modem.	RJ-45	10/100 Mbps/ Ethernet
Ports 1-4	Enables direct connections to workstations or a LAN connection through a switch or hub. Use this connection to manage the device through a Telnet session or the WebUI management application.	RJ-45	10/100 Mbps/ Ethernet

Status LEDs

The front panel of the NetScreen-Hardware Security Client device has power and status LEDs for the device, and port status LEDs for the interfaces:



Interpreting Power & Status LEDs

The power status LED indicates whether the device is receiving power and the status LED indicates the state of the device. The following table describes the status possibilities for each LED:

LED	LED Color	Meaning of the LED
POWER	Green	Solid On indicates the system is receiving power
	Off	Off indicates the system is not receiving power.
STATUS	Amber	Solid On indicates the system is not communicating to NMS.
	Green	Blinking On indicates the system is functioning.
	Amber	Blinking On indicates a factory default or a failed upgrade.
	Off	Off indicates the system is not operational.

Interpreting Port Status LEDs

The port status LEDs indicate whether the ports on the device are operating properly. The following table describes the status possibilities for the ports.

LED	LED Color	Meaning of the LED
Link/Activity	Green	Blinking On indicates the device detects Ethernet traffic for the port.
		Off indicates the port has not established a link with another device.
		Solid On indicates the port has established a link with another device.
10/100	Green	Solid On indicates the port is connected to a 100 Base-T device.
	Amber	Solid On indicates the port is connected to a 10 Base-T device.

A

Specifications

This appendix provides general system specifications for the Juniper Networks NetScreen-Hardware Security Client.

Attributes		
Height	1.125 inches (2.858 cm)	
Depth	5 inches (12.7 cm)	
Width	8.25 inches (20.955 cm)	
Weight	1.3 pounds (590g)	
Electrical	Switching Regulator	Linear Regulator
	AC voltage: 100-240 VAC +/- 10% 50/60 Hz AC Watts: 12 Watts DC voltage: 12 Volts	AC voltage: 120 VAC +/- 10% 50/60 Hz AC Watts: 12 Watts DC voltage: 12 Volts
Environmental	Temperature	Operating
	Normal altitude	0°-40° C, 32-105°F
	Relative humidity	10-90%
	Non-condensing	10-90%
Certifications	Safety	EMI
	UL/CUL CB CSA 6950 EN 60950 IEC 60950 PSE-Mark (T-Mark) External Power Supply	CE Class B FCC Part 15 class B CTICK BSMI VCCI Class II Austel
Connectors	The RJ-45 twisted-pair ports are compatible with the IEEE 802.3 Type 10/100 Base-T standard	
Standard	100Base-TX	
Media Type	Category 5 and higher Unshielded Twisted Pair (UTP) Cable	
Maximum Distance	109.361 yards (100 m)	